

U.S. Department of State, Information Resource Management,  
Office of Information Assurance, October 5, 2010

# **FISMA 2.0: Risk Valuation, Time and Results**

---



John Streufert ( [DOSCISO@state.gov](mailto:DOSCISO@state.gov) )  
Deputy Chief Information Officer for Information Security  
US Department of State  
October 5, 2010

# FISMA 1.0

On December 17, 2002, the President signed into law the Electronic Government Act. Title III of that Act is FISMA, which *lays out the framework for annual IT security reviews, reporting, and remediation planning at federal agencies.* It requires that agency heads and IGs evaluate their agencies' computer security programs and report the results of those evaluations to OMB, Congress, and the GAO. <sup>1</sup>

<sup>1</sup> House Oversight and Government Reform website

# FISMA Today

## OMB directs “*snapshots*” of process and compliance

1. “**Annual**” systems inventory
2. “**Annual**” testing
3. C&A<sup>⌘</sup> every “**three**” years
4. Weaknesses “**Quarterly**”
5. Train “**once a year**”  
(awareness)

⌘ Certification and Accreditation studies

# FISMA 2.0 Target

## Continuous:

7. Incident Reporting
6. Configuration Management
5. “Daily” weakness updates
4. C&A technical controls **x 72** <sup>⌘</sup>
3. **Daily** not “Annual” testing
2. **Inventory** improvements
1. “Daily” awareness training

⌘

Certification and Accreditation study of technical controls

# RISK

**Threat**



**Vulnerabilities**

**Impact**

# Threats Increase

## TICKETS

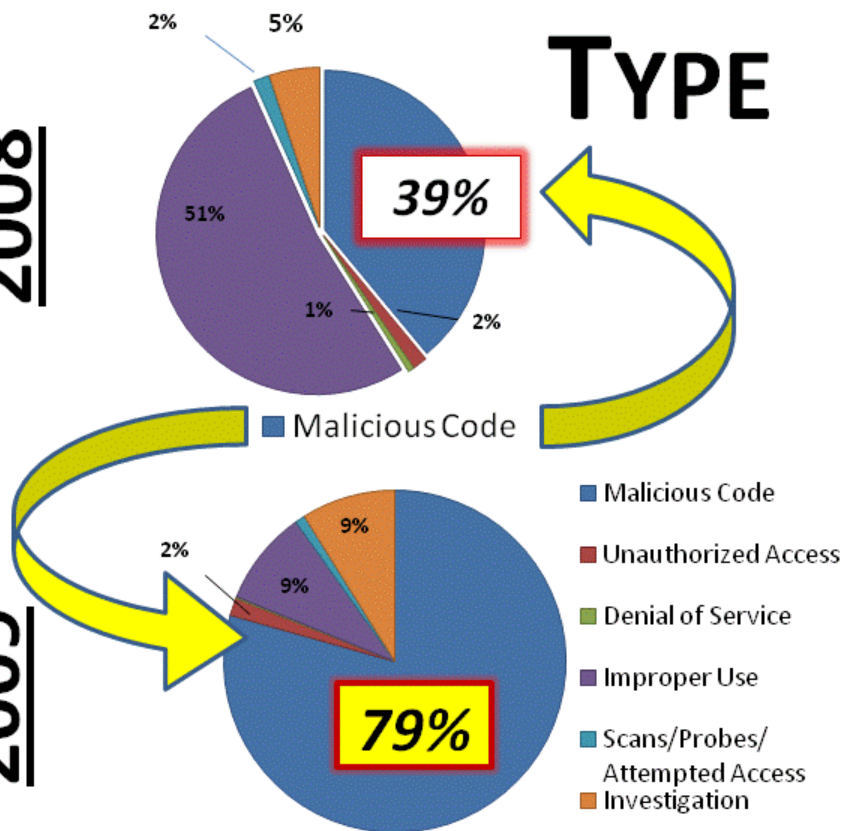
Years	Tickets
2008	2104
2009	3085
2010	+6000 * projected

\* 3000 by June 2010

2008

2009

## TYPE



# Nature of Attacks

80% of attacks leverage  
known vulnerabilities and  
configuration management  
setting weaknesses

# **“Attack Readiness”**

- What time is spent on
- Faster action =  
lower potential risk



# Risk Valuation

# Bad Things By The Numbers

## Littering



## Chemical Dumping

-- L.A. Hotel Fined --

---

Hotel pays a

**\$200,000 fine**

because an employee dumps  
pool chemicals into a drain  
fumes fill a subway station  
-- several people become ill

March 23, 2010

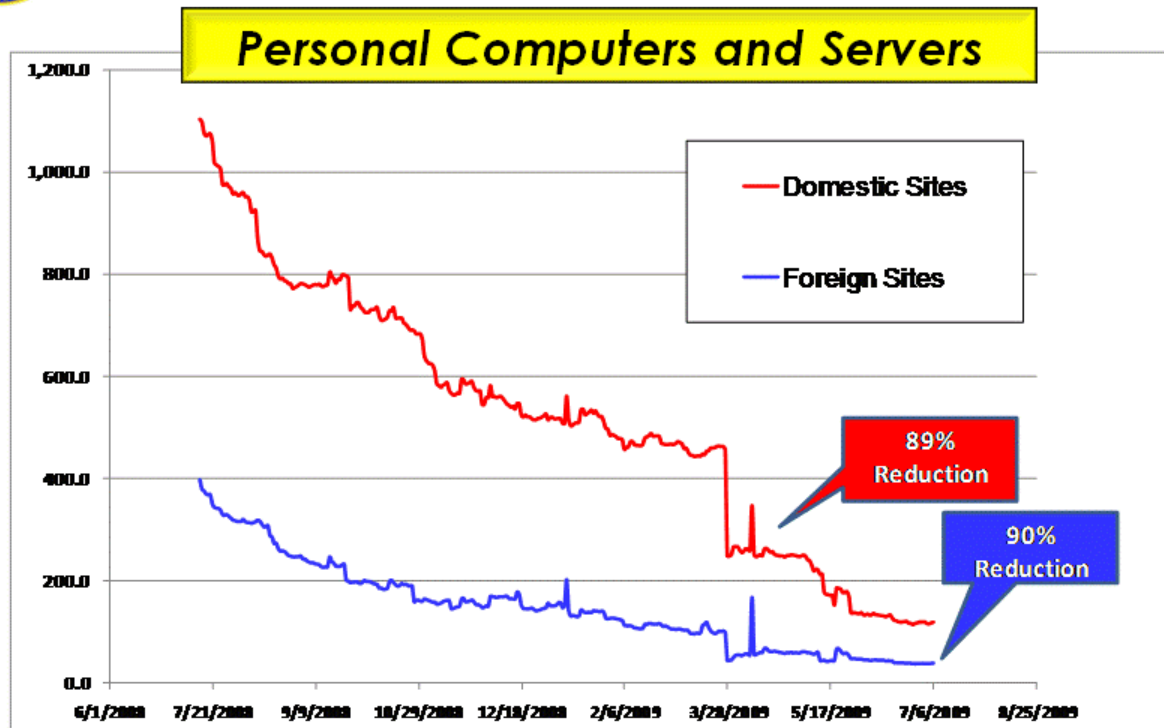


# Case Study:

- (1) Scan every 2 – 15 days
- (2) Find & Fix Top Issues Daily
- (3) Personal results graded
- (4) Hold managers responsible

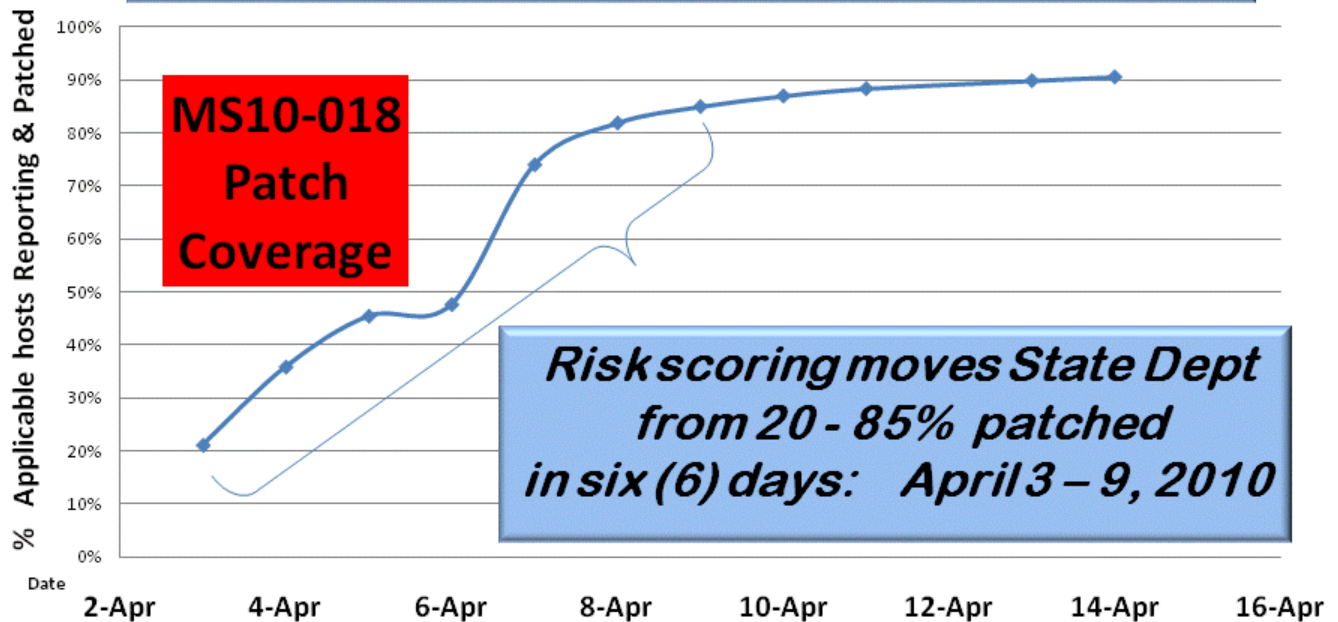


# Results First 12 Months

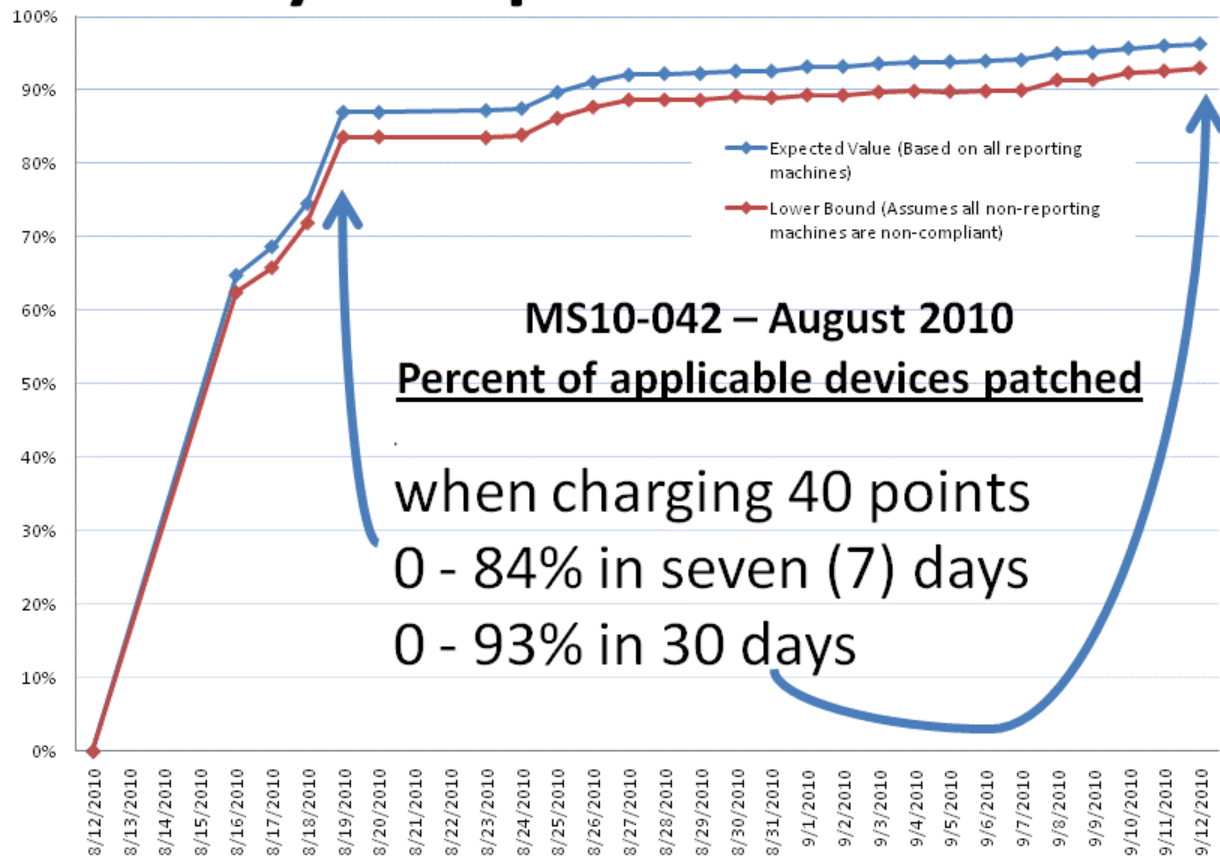


# Call a Problem 40x Worse

## *Operation Aurora Attack*



# Efficiency is Repeatable & Sustained



**Why  
and  
How?**

# OBSTACLE

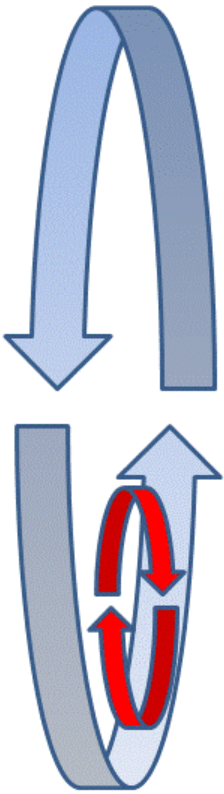
---

CXOs are **accountable** for IT security

**BUT**

**directly supervise only  
a small part of the  
systems actually in use.**





# Tactical Problem

- In combat whoever “Observes – Orients – Decides – Acts”<sup>1</sup> fastest wins.
- Cyber attacks are evolving faster than they can be counteracted outside DoD

<sup>1</sup> ‘OODA’ loops described in Boyd , The Fighter Pilot Who Changed the Art of War, by Robert Coram

# **Structuring for Success**






# #1: Narrow Aim

CAG ID	Consensus Audit Guideline	NIST-800-53	US CERT Report
1	Inventory of authorized and unauthorized hardware	CM-1, CM-2, CM-3, CM-4, CM-5, CM-8, CM-9	[11 months before Feb 09] <b>+ 6 %</b>
2	Inventory of authorized and unauthorized software	CM-1, CM-2, CM-3, CM-5, CM-7, CM-8, CM-9, SA-7	<b>+ 22 %</b>
5	Boundary Defense	AC-17, RA-5, SC-7, SI-4	<b>+ 7 %</b>
9	Controlled access based on need to know	AC-1, AC-2, AC-3, AC-6, AC-13	<b>1 %</b>
12	<b>Anti-malware defenses</b>	AC-3, AC-4, AC-6, AC-17, AC-19, AC-20, AT-2, AT-3, CM-5, MA-3, MA-4, MA-5, MP-2, MP-4, PE-3, PE-4, PL-4, PS-6, RA-5, SA-7, SA-12, SA-13, SC-3, SC-7, SC-11, SC-20, SC-21, SC-22, SC-23, SC-25, SC-26, SC-27, SC-29, SC-30, SC-31, SI-3, SI-8	<b>+ 60%</b>

# **#2: Set Metrics**

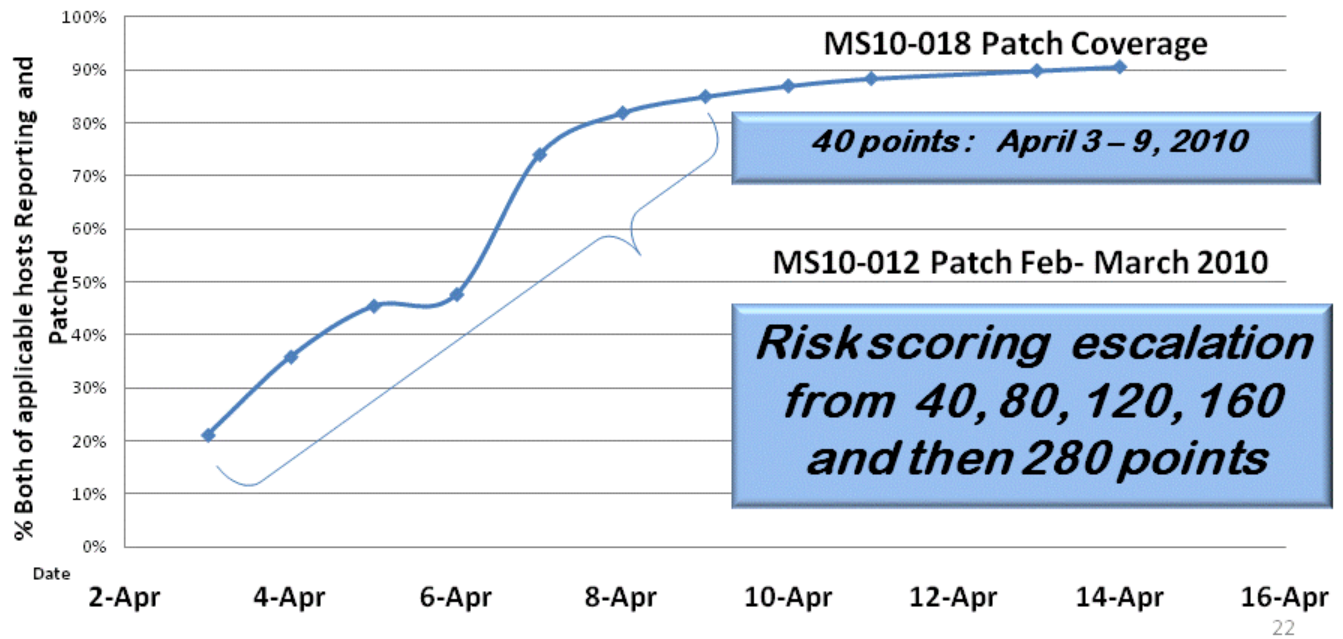
Quantify risk for action:

**a. Name common standards**

Component	Risk Score	Avg / Host	% of Score	How Component is Calculated
VUL - Vulnerability 	947.0	3.0	10.9 %	From .1 for the lowest risk vulnerability to 10 for the highest risk vulnerability
PAT - Patch	603.0	1.9	6.9 %	From 3 for each missing "Low" patch to 10 for each missing "Critical" patch
SCM - Security Compliance 	6,181.2	19.5	71.2 %	From .9 for each failed Application Log check to .43 for each failed Group Membership check
AVR - Anti-Virus	0.0	0.0	0.0 %	6 per day for each signature file older than 6 days
SOE - SOE Compliance	115.0	0.4	1.3 %	5 for each missing or incorrect version of an SOE component
ADC - AD Computers	26.0	0.1	0.3 %	1 per day for each day the AD computer password age exceeds 35 days
ADU - AD Users	222.0	0.7	2.6 %	1 per day for each account that does not require a smart-card and whose password age > 60, plus 5 additional if the password never expires
SMS - SMS Reporting	230.0	0.7	2.6 %	100 + 10 per day for each host not reporting completely to SMS
VUR - Vulnerability Reporting	84.0	0.3	1.0 %	After a host has no scans for 15 consecutive days, 5 + 1 per 7 additional days
SCR - Security Compliance Reporting	279.0	0.9	3.2 %	After a host has no scans for 30 consecutive days, 5 + 1 per 15 additional days
<b>Total Risk Score</b>	<b>8,687.1</b> 	<b>27.4</b> 	<b>100.0 %</b> 	
<p><i>For additional information on Risk Scoring, assistance with remediations, or to report suspected false positives, contact the IT Service Center to open a "Risk Score" ticket.</i></p>				

## b. Quantify Unique Threats

### *Google - Aurora Attack*



# #3: Focus Gains

## Technical control data efficiency:

- Every **2-15 days** not **3 years**

## Create tiger teams for operations:

- inventory and to reduce site risks

## C&A<sup>✕</sup> cost down **56% then 62%**

- Invest in tool kits for everything  
Support just in time for Certification & Accreditation<sup>✕</sup>

# #4: Right Tools

---

## *Integrate Information & Tools*

Timely – Targeted<sup>2</sup> – Prioritized

*“Metrics with  
the Most Meaning”*

<sup>2</sup> The One to One Fieldbook: The Complete Toolkit for Implementing a 1 to 1 Marketing Program by [Don Peppers](#), [Martha Rogers](#), and [Bob Dorf](#)



# **#5 Embed Time & Results Checks into Daily Operations**

## Site Filter Options:

Foreign Domestic

Abidjan

## Performance

Server Performance

Network Latency

Network Traffic

Network Usage

Performance Alerts

## Security

Compliance Scans

Vulnerability Scans

Active Directory

Patch Management

## Configuration

Processor

Memory

Logical Disk

## Risk Scoring Reports

[All Risk Scoring Exceptions](#)**Enterprise Level**

Enterprise and local risk scoring exceptions.

[Vulnerability Management](#)**Enterprise Level**

Active scoring exceptions for vulnerabilities

[Risk Score Rank](#)**Site Level**

Displays site risk score ranks in the enterprise

[Enterprise Risk Score Monitor](#)**Enterprise Level**

Risk scores, grades, and rankings for each primary site in the Enterprise

[Regional Risk Score Monitor](#)**Regional Level**

Risk scores, grades, and rankings for each site

[Risk Scoring Exceptions](#)**Site Level**

Risk scoring exceptions applicable to the selected site

[Site Collection Risk Score Monitor](#)**Enterprise Level**

Risk scores, grades, and rankings for each site in a named site collection

[Risk Score Advisor](#)**Site Level**

Analysis assistance to facilitate improvement of risk score

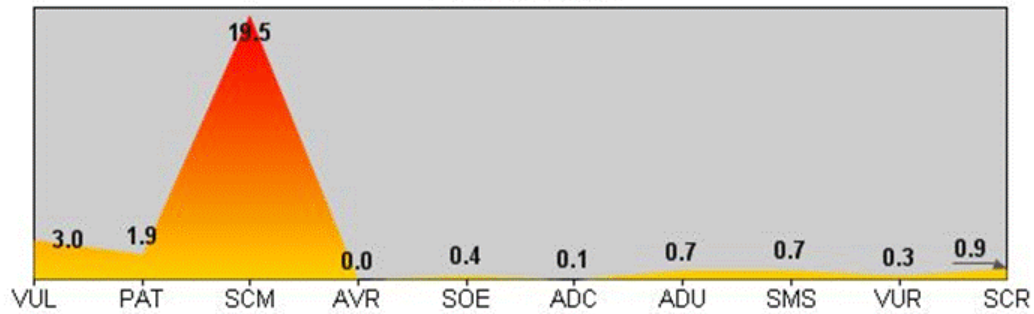
## Risk Score Advisor

The following grading scale is provided by Information Assurance and may be revised periodically.

Site Risk Score	8,687.1
Hosts	317
Average Risk Score	27.4
Risk Level Grade	A+
Rank in Enterprise	163 of 438
Rank in Region	16 of 48

Average Risk Score		
At Least	Less Than	Grade
0.0	40.0	A+
40.0	75.0	A
75.0	110.0	B
110.0	180.0	C
180.0	280.0	D
280.0	400.0	F
400.0	-	F-

Risk Score Profile

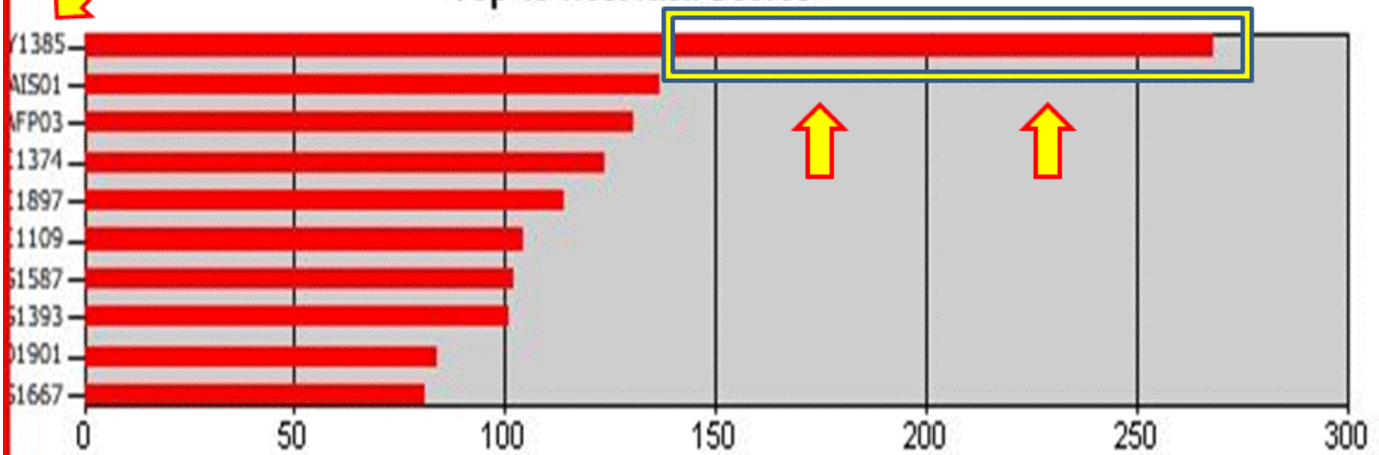


Component	Risk Score	Avg / Host	% of Score	How Component is Calculated
VUL - Vulnerability	947.0	3.0	10.9 %	From .1 for the lowest risk vulnerability to 10 for the highest risk vulnerability
PAT - Patch	603.0	1.9	6.9 %	From 3 for each missing "Low" patch to 10 for each missing "Critical" patch
SCM - Security Compliance	6,181.2	19.5	71.2 %	From .9 for each failed Application Log check to .43 for each failed Group Membership check
AVR - Anti-Virus	0.0	0.0	0.0 %	6 per day for each signature file older than 6 days
SOE - SOE Compliance	115.0	0.4	1.3 %	5 for each missing or incorrect version of an SOE component
ADC - AD Computers	26.0	0.1	0.3 %	1 per day for each day the AD computer password age exceeds 35 days
ADU - AD Users	222.0	0.7	2.6 %	1 per day for each account that does not require a smart-card and whose password age > 60, plus 5 additional if the password never expires
SMS - SMS Reporting	230.0	0.7	2.6 %	100 + 10 per day for each host not reporting completely to SMS
VUR - Vulnerability Reporting	84.0	0.3	1.0 %	After a host has no scans for 15 consecutive days, 5 + 1 per 7 additional days
SCR - Security Compliance Reporting	279.0	0.9	3.2 %	After a host has no scans for 30 consecutive days, 5 + 1 per 15 additional days
<b>Total Risk Score</b>	<b>8,687.1</b>	<b>27.4</b>	<b>100.0 %</b>	

*For additional information on Risk Scoring, assistance with remediations, or to report suspected false positives, contact the IT Service Center to open a "Risk Score" ticket.*



### Top 10 Host Risk Scores



### Risk Score History



## Site Filter Options:

☒ Foreign ☐ Domestic

Abidjan

## Performance

- Server Performance
- Network Latency
- Network Traffic
- Network Usage
- Performance Alerts

## Security

- Compliance Scans
- Vulnerability Scans
- Active Directory
- Patch Management

## Configuration

- Processor
- Memory
- Logical Disk

## Risk Scoring Reports

 [All Risk Scoring Exceptions](#)**Enterprise Level**

Enterprise and local risk scoring exceptions.

 [Vulnerability Management](#)**Enterprise Level**

Active scoring exceptions for vulnerabilities

 [Risk Score Rank](#)**Site Level**

Displays site risk score ranks in the enterprise

 [Enterprise Risk Score Monitor](#)**Enterprise Level**

Risk scores, grades, and rankings for each primary site in the Enterprise

 [Regional Risk Score Monitor](#)**Regional Level**

Risk scores, grades, and rankings for each site

 [Risk Scoring Exceptions](#)**Site Level**

Risk scoring exceptions applicable to the selected site

 [Site Collection Risk Score Monitor](#)**Enterprise Level**

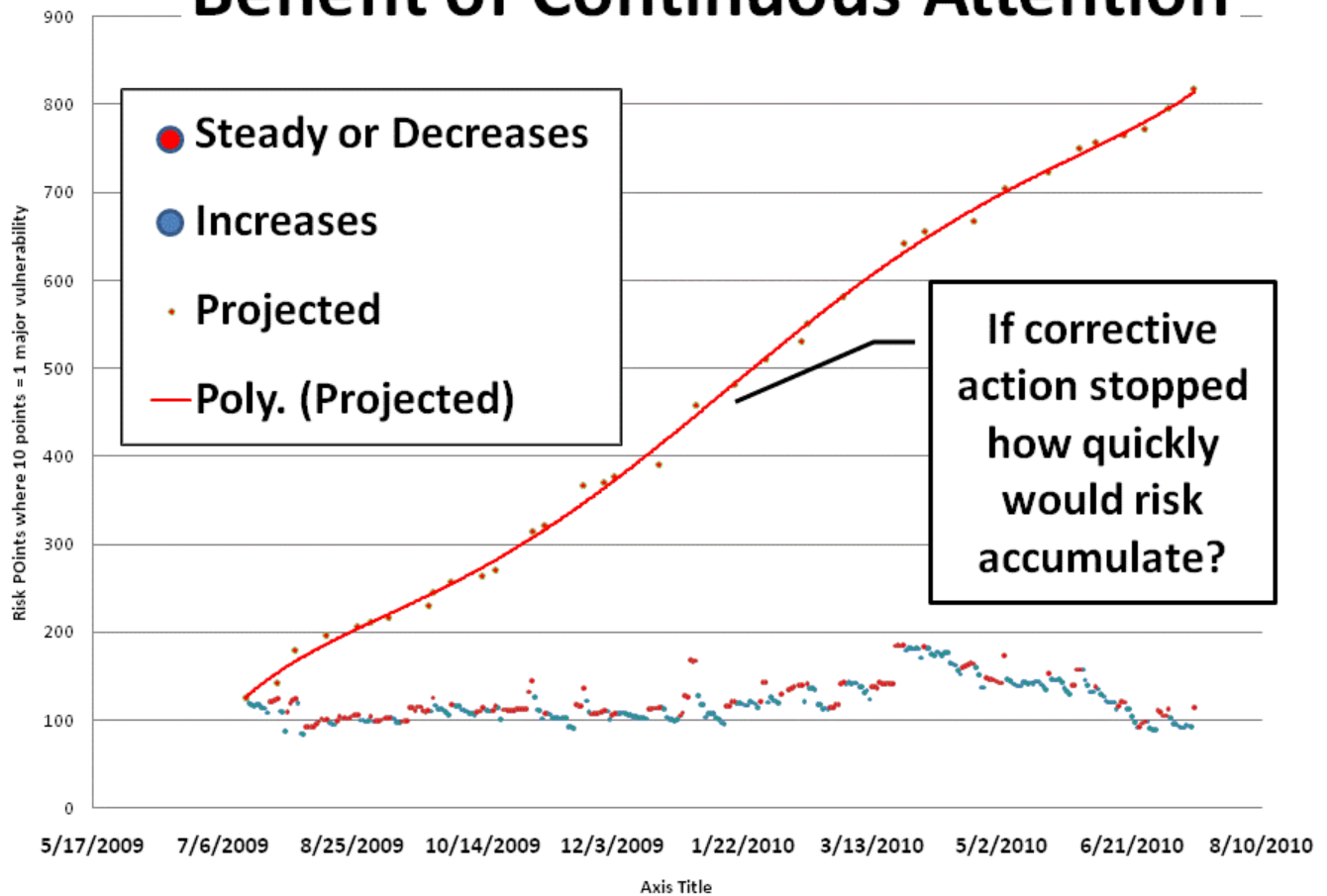
Risk scores, grades, and rankings for each site in a named site collection

 [Risk Score Advisor](#)**Site Level**

Analysis assistance to facilitate improvement of risk score

# **#6 Assure Ongoing Accountability and Continuous Improvement**

# Benefit of Continuous Attention





# Risk Score Monitor Enterprise

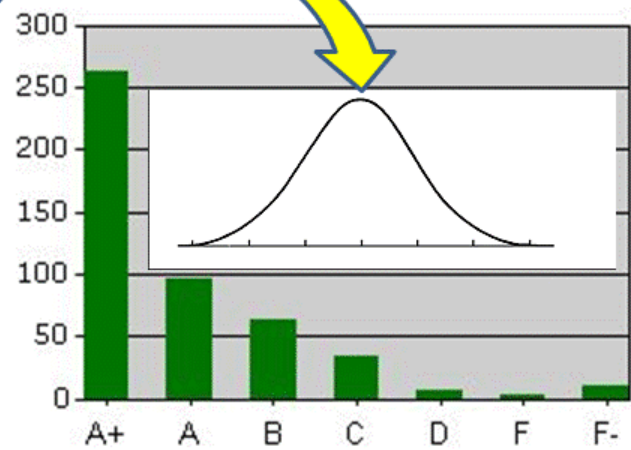
Total Hosts	32,366	51,157
Average Risk Score per Host	101.7	33.2

## Grading Scale

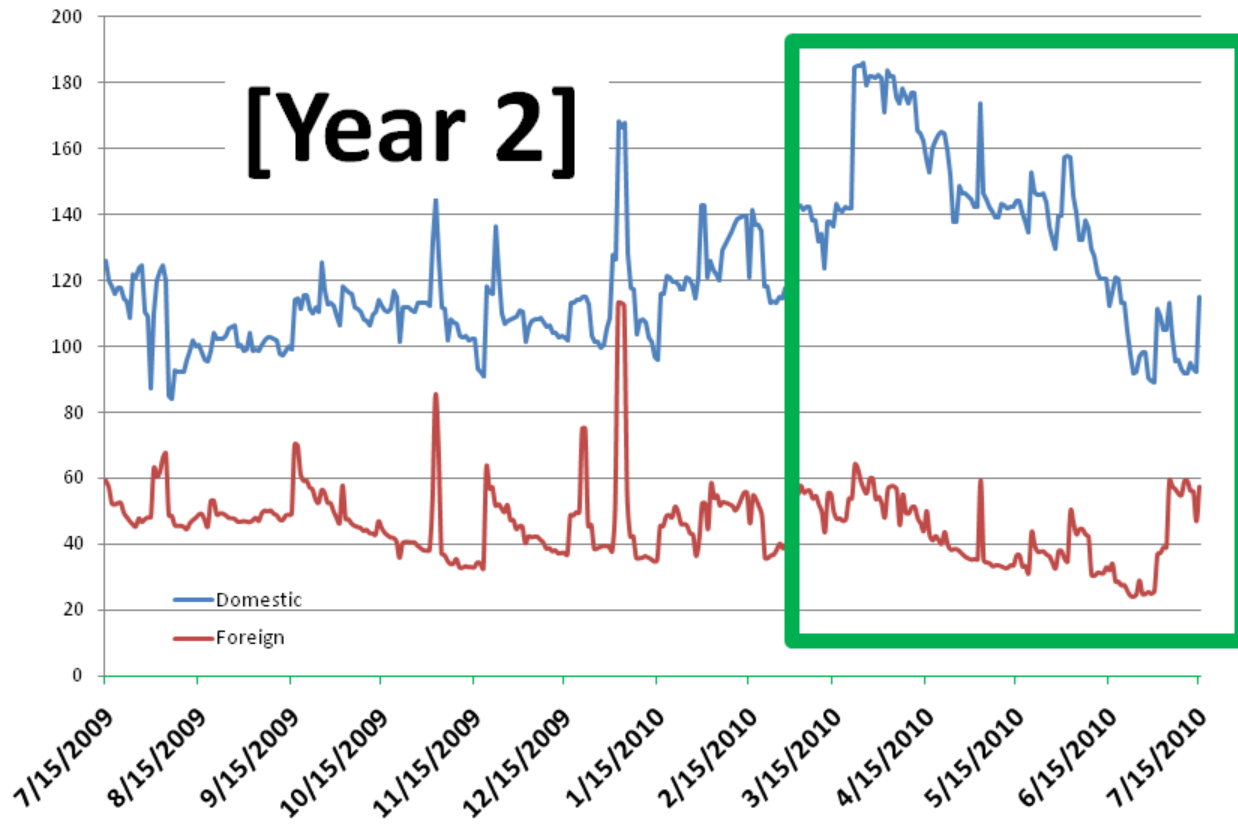
Average Risk Score			
At Least	Less Than	Grade	
0.0	40.0	A+	13
40.0	75.0	A	25
75.0	110.0	B	36
110.0	180.0	C	60
180.0	280.0	D	93
280.0	400.0	F	133
400.0		F-	

# Sites

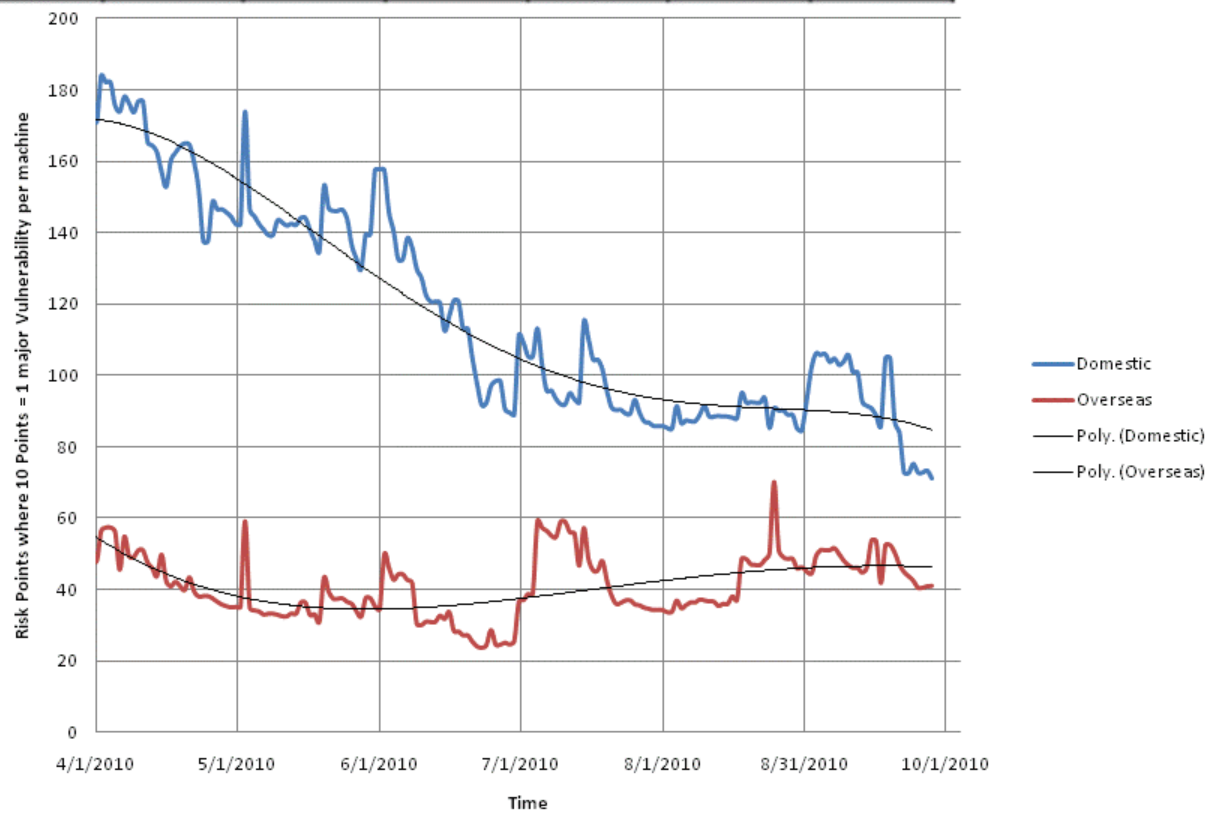
## Grade Dis



# 1/3 of Remaining Risk Removed



Grade	Now	April	May	June	July	Aug	Sep
A+	40	36	31	27	22	18	13



# **#7 Design to Test**

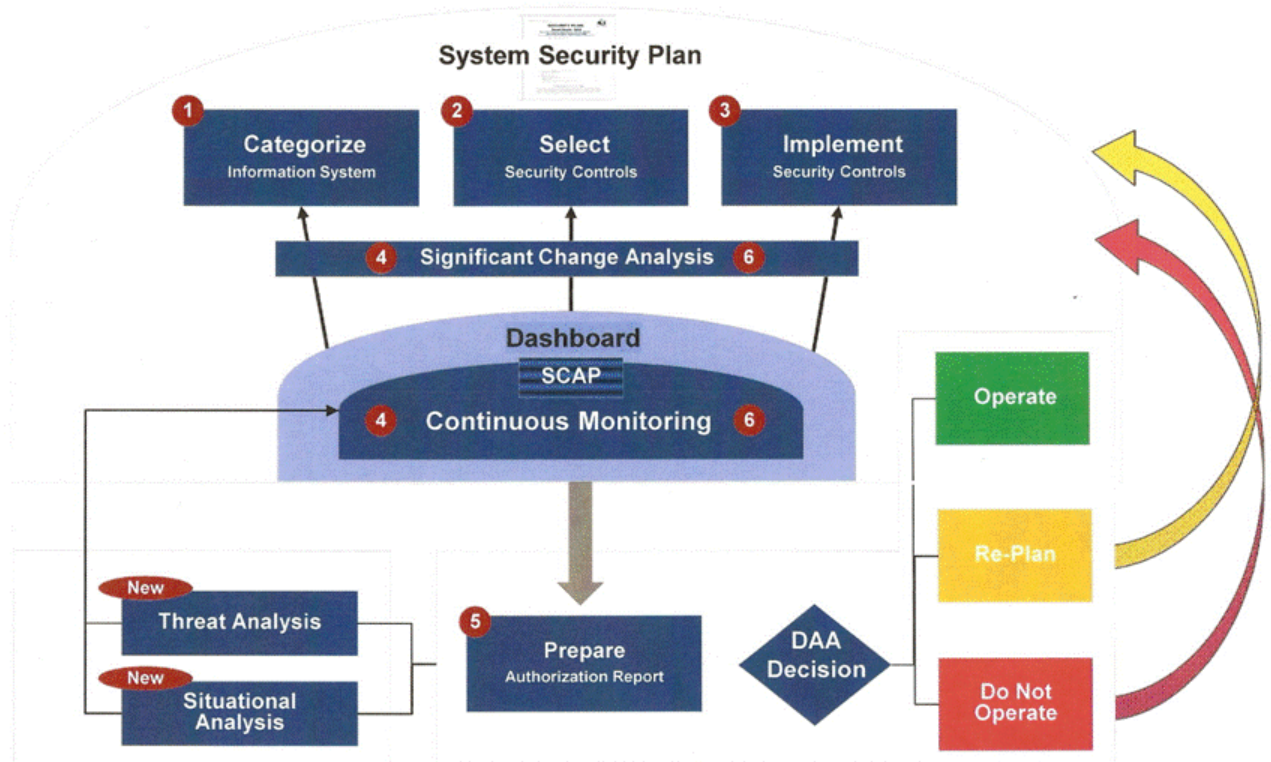
# Should we position our best solutions before or after accidents?



Cofferdam unit departing Wild West in Port Fourchon on the Chouest 280 workshop named Joe Griffin 05 May 2010 -- Photo from BP.com

# Continuous C&A Process will provide more effective real-time security – not just a snapshot in time

## Continuous C&A Process



# Finding

**Details empower  
technical managers**

*FOR TARGETED, DAILY  
ATTENTION TO REMEDIATION*

**Summaries  
empower executives**

*TO OVERSEE CORRECTION OF  
MOST SERIOUS PROBLEMS*

# Lessons Learned

- When **continuous monitoring** augments snapshots required by FISMA:
  - Mobilizing to lower risk is feasible & fast (11 mo)
  - Changes in 24 time zones with no direct contact
  - Cost: 15 FTE above technical management base
- This approach leverages the wider workforce
- Security culture gains are grounded in fairness, commitment and personal accountability for improvement



# Conclusions

- Scalable to large complex public and private sector organizations
- Higher ROI for continuous monitoring of technical controls as a substitute for paper reports
- Summarized risk estimates could be fed to enterprise level reporting

# Background

# Steps at the State Department

***Continuous Certification & Accreditation  
Pilot and contracts Summer 2010***

***1<sup>st</sup> Year: State Measures 89% risk reduction – July 09***

***Enterprise pilot test on servers/PC's begins – July 08***

***C&A Cost reduced 56%, then to 62% with Toolkits - 2007***

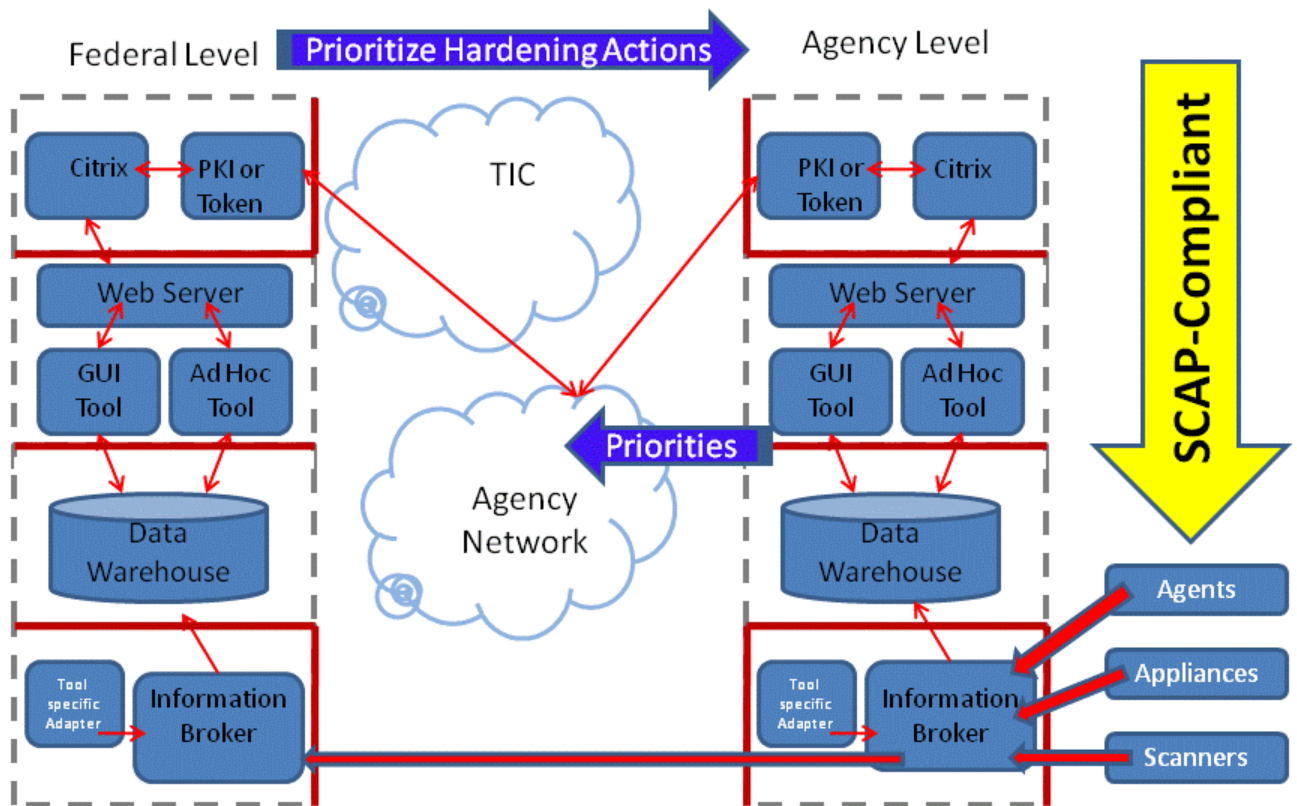
***Coalition for grading better cyber risk - State 2006***

***COTS Vulnerability & Config Mang Scanner – State 2005***

***Grades A-F Use Risk Points + Letters to Execs – USAID 2004***

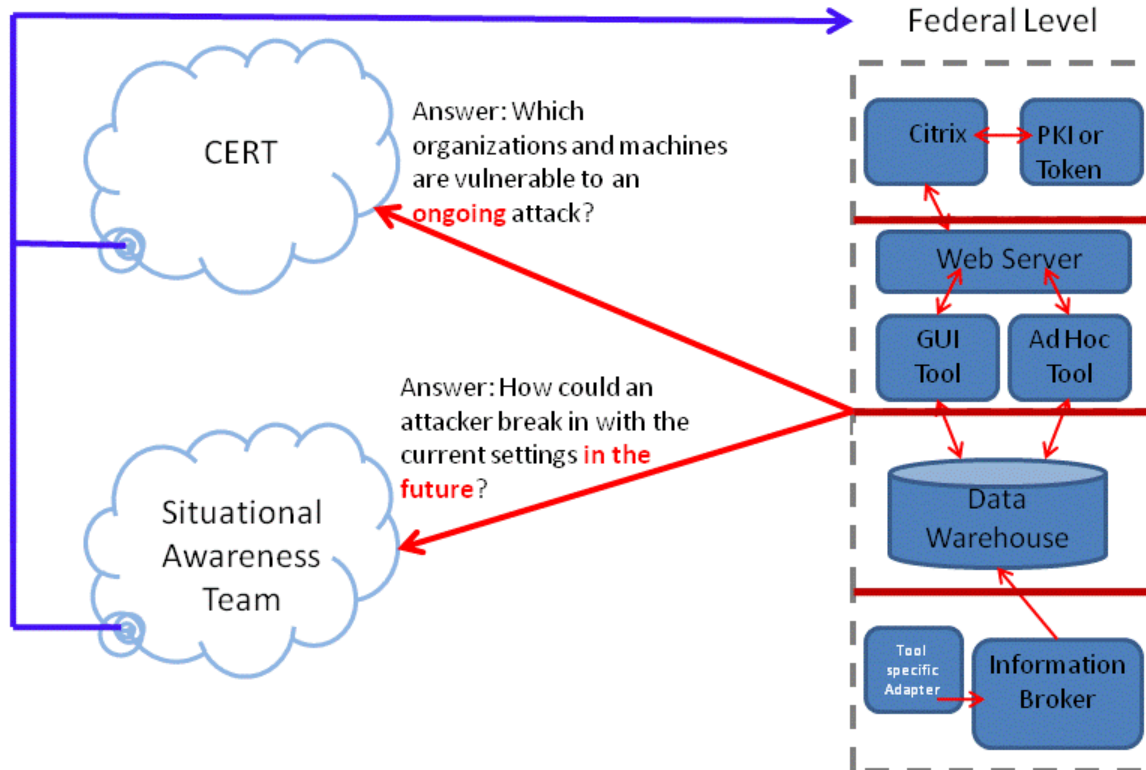
***Increase Scanning to Every 3 Days – USAID late FY 2003***

# Architecture



# Integration (& Impact)

Answer: Adjust priorities for hardening in response to actual/possible threats



# Training

Tips of the Day Application

Security Tip of the Day [options](#)  
[help/comment](#)

---



Is your classified media “secured?”

Removable hard drives containing classified information must be locked in an approved safe after you finish using them!

**Classified media aren’t “secured” until they are locked in an approved safe.**

---

If I leave my computer for any reason, I must secure all removable media that contain CLASSIFIED information.

[view my results](#)

# For further information the following POCs

## Points of Contact

John Streufert  
Chief Information Security Officer



Department of State, IRM/IA  
Arlington, VA 22209  
Tel (703) 812-2555  
[streufertj@state.gov](mailto:streufertj@state.gov)

George Moore  
Chief Computer Scientist



Department of State, IRM/IA  
Arlington, VA 22209  
Tel (703) 812-2209  
[mooregc@state.gov](mailto:mooregc@state.gov)

Pete Gouldmann  
NIST & CNSS Liaison



Department of State, IRM/IA  
Arlington, VA 22209  
Tel (703) 812-2201  
[gouldmannp@state.gov](mailto:gouldmannp@state.gov)

Sara Mosley  
Senior Security Engineer



Department of State, IRM/IA  
Arlington, VA 22209  
Tel (703) 812-2555  
[mosleyss@state.gov](mailto:mosleyss@state.gov)